

(43) 国際公開日
2006 年 4 月 27 日 (27.04.2006)

PCT

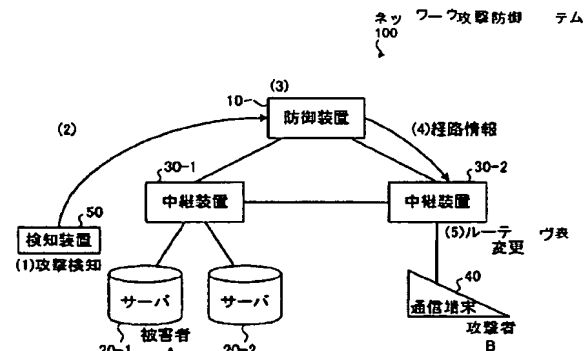
(10) 国際公開番号
WO 2006/043371 A1

- (51) 国際特許分類:
H04L 12/66 (2006.01) G06F 1/30 (2006.01)
H04L 12/56 (2006.01)
- (21) 国際出願番号: PCT/JP2005/0 16554
- (22) 国際出願日: 2005 年 9 月 8 日 (08.09.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (50) 優先権子タ:
特 許 2004-306533
2004 年 10 月 21 日 (21.10.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP], 〒1008116 東京都千代田区大手町二丁目 3 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 倉上 弘 (KURAKAMI, Hiroshi) [JP/JP], 〒1808585 東京都武蔵野市緑町 3 丁目 9 - 1 1 N T T 知的財産センタ内 Tokyo (JP). 瀬林 克啓 (SEBAYASHI, Katsuhiko) [JP/JP], 〒1808585 東京都武蔵野市緑町 3 丁目 9 - 1 1 N T T 知的財産センタ内 Tokyo (JP). 佐竹 康宏 (SATAKE, Yasuhiro) [JP/JP], 〒1808585 東京都武蔵野市緑町 3 丁目 9 - 1 1 N T T 知的財産センタ内 Tokyo (JP).
- (74) 代理人: 酒井 宏明 , 外 (SAKAI, Hiroaki et al) 〒1006019 東京都千代田区霞が関三丁目 2 番 5 号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KP, KR, KZ, LC, LK,

[続葉有]

(54) Title: PROTECT DEVICE, PROTECT METHOD, PROTECT PROGRAM, AND NETWORK ATTACK PROTECT SYSTEM

(54) 発明の名称: 防御装置、防御方法および防御プログラム並びにネットワーク攻撃防御システム



100 NETWORK ATTACK PROTECT SYSTEM
 (3) RELAY DEVICE SELECT
 10 PROTECT DEVICE
 (2) ATTACK INFORMATION
 30 1 R LAY D VICE
 50 DE ECT DEVICE
 (1) ATTACK ETECT

20 1 SERVER
 A VICTIM
 20 2 SERVER
 (4) ROUTE INFORMATION
 30 2 R LAY D VICE
 (5) ROUTING ABLE CHANGE
 40 COMMUNICATION TERMINAL
 B ATTACKER

(57) Abstract: In response to attack information from a detect device (50), a protect device (10) determines, in case it specifies a server (20-1) being attacked from the attack information, a relay device (30-1) to become a next relay target for the specified server (20-1), from a routing table, and selects such a relay device (30-2) from the relay device (30-1) and the relay device (30-2) adjoining the protect device (10) as excludes the relay device (30-1), as a notice target. The protect device (10) notifies the relay device (30-2) selected, of the route information for passing an attack packet to itself, and controls the passage of the attack packet passed to itself from the relay device (30-2), for which the routing table was changed, on the basis of that route information.

要約: 防御装置 10 は、検知装置 50 から攻撃情報を受信すると、攻撃情報から攻撃を受けているサーバ 20-1 を特定した場合には、特定したサーバ 20-1 に対して次の中継先となる中継装置 30-1 をルーティング表から求め、防御装置 10 と隣接する中継装置 30-1 および中継装置 30-2 のなかから、この

[続葉有]

WO 2006/043371 A1



LR, LS, LT, LU, LV, MA, MD, MG, 1k, MN, MW, MX,
MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU,
SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, V#J, YU, ZA, ZM, ZW

IS, IT, LT, LU, LV, MC, NL, PL, PT, Rø, SE, SI, SK, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), -x-ラシT (AM, AZ, BY, KG, KΔ MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

添付公開書類:

- 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

中継装置30-1を除いた中継装置30-2を通知先として選択する。そして、防御装置10は、選択した中継装置30-2に対して、攻撃パケットを自己に経由させるための経路情報を通知し、かかる経路情報に基づいてルーティング表を変更した中継装置30-2から自己に経由されてきた攻撃パケットの通過を制御する。